

CERIAS

The Center for Education and Research in Information Assurance and Security

The Effects of Online Anxiety on Cyber-Hygiene

Sunjae Choi, Tatyana Tsyganyuk, Subia Ansari, Priyanka Tiwari, Ida Ngambeki
Purdue University

The Problem

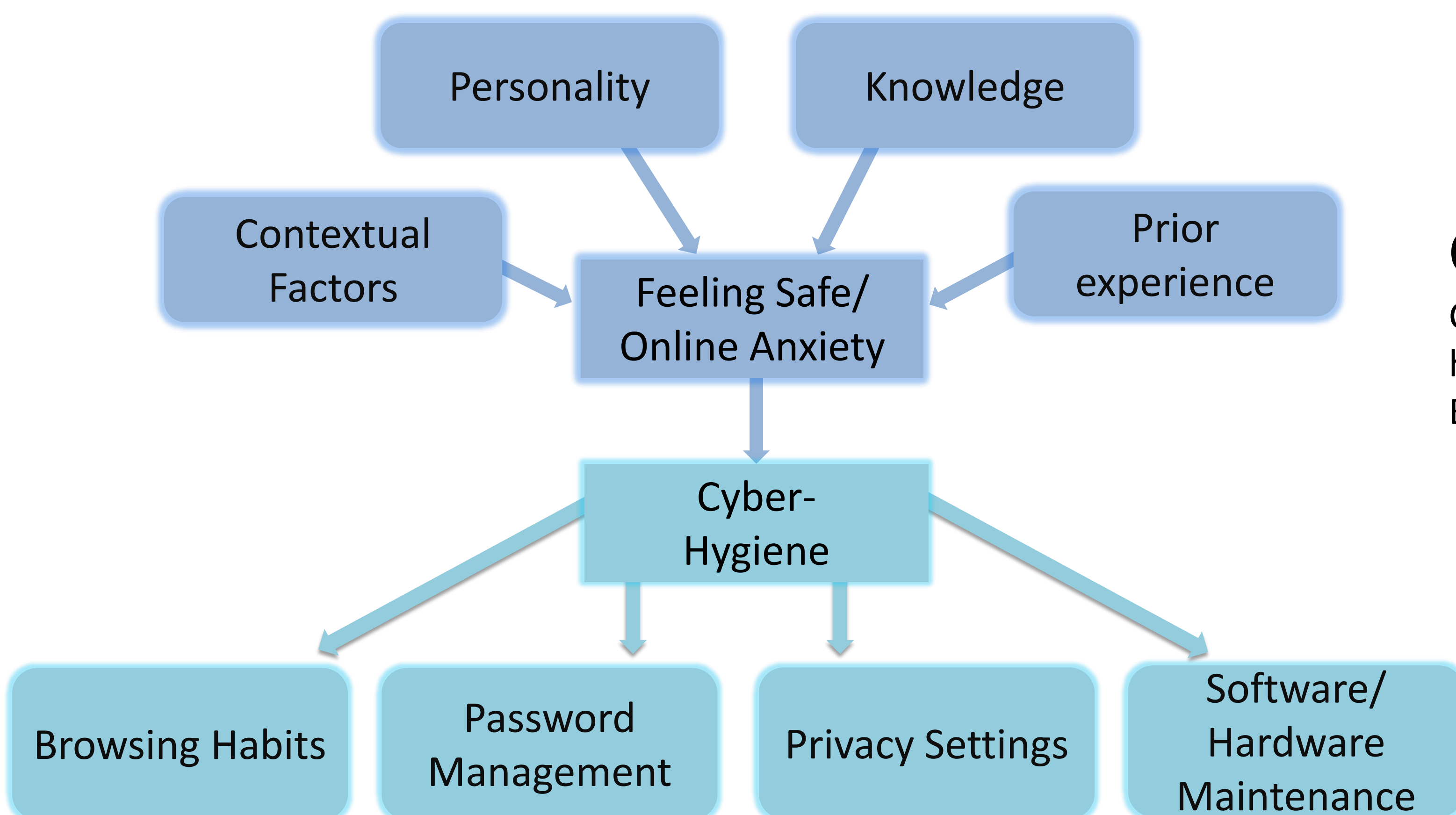
There is a lack of basic cybersecurity knowledge among the majority of the population. The majority of cybersecurity education is not tailored to fundamental and novice users.

Research Questions

- What factors affect the adoption of cyber-secure attitudes and behaviors
- What level of cyber-hygiene do people regularly engage in?
- Do positive/negative experiences online have a mediating effect on cyber-hygiene?

Method

A survey was developed to measure each of the constructs identified. Data were collected using Amazon Mturk (N=300)



Online Anxiety

Computer anxiety is the fear of using a computer. It has been found to be fairly prevalent, occurring in 30-40% of people (Buche, Davis & Vician, 2007). It has been found to affect individual's willingness to engage with and learn about computers. Online anxiety is believed to be related and the result of:

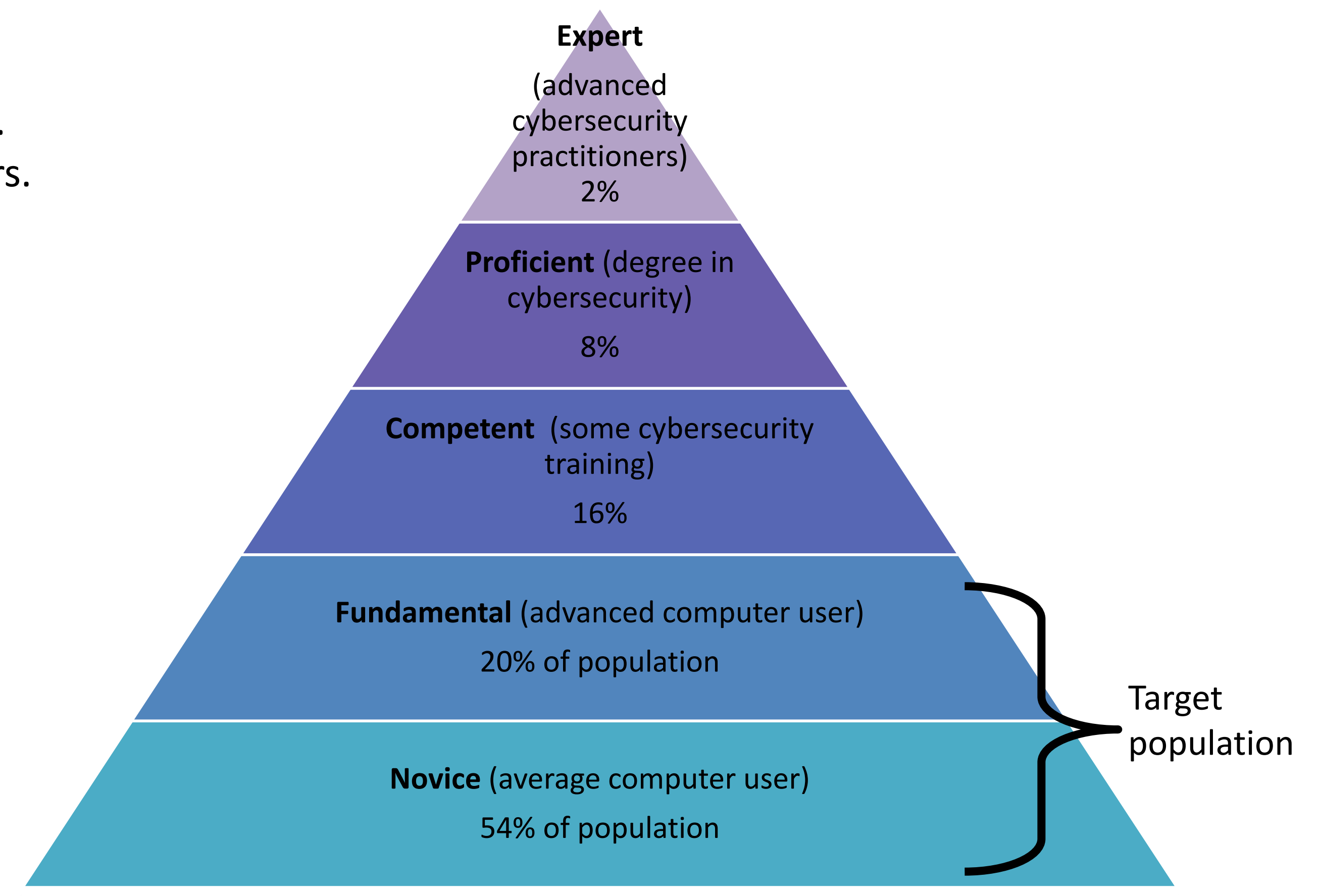
- Lack of knowledge
- Fear of making a mistake
- Lack of self-efficacy

Results

- 85% of the population experienced above average anxiety
- 89% engage in basic cyber-hygiene
- Only 26% engage in more rigorous cyber-hygiene
- There is a significant difference by ethnicity in who engages in cyber-hygiene [$F(6,289) = 2.703, p = 0.01$]
- There was a correlation between feeling safe online and cyber-hygiene [$r = 0.268, n = 284, p < 0.001$] suggesting that people who experienced less anxiety online had better cyber-hygiene.
- There was a negative correlation between risk taking behavior and good cyber-hygiene [$r = -.31, n = 294, p < .001$] suggesting that people who take higher risks are more likely to have poor cyber-hygiene.

References

Buche, Mari & Davis, Larry & Vician, Chelley. (2007). A Longitudinal Investigation of the Effects of Computer Anxiety on Performance in a Computing-Intensive Environment. Journal of Information Systems Education. 18.



Cyber-Hygiene

Cyber hygiene refers to the practices that users should take to maintain the health and security of their computers and other devices.

Best practices include:

- Regular software updates
- Regular hardware updates
- Back up all data
- Password management (strong passwords/pass phrases, unique to each account, changed regularly)
- Implement two-factor authentication
- Install anti-malware/anti-virus
- Keep an inventory of hardware and software
- Implement access control
- Be vigilant for phishing emails and unsecured websites

Basic Cyber-hygiene behavior

